Securing Mobile and Wireless Networks

Will Ivancic

wivancic@grc.nasa.gov

216-433-3494

Outline

- Network Security, What is it?
- Security Truths
- Mobile and Wireless Networks
- Issues / Challenges
- USCG/NASA/Cisco Neah Bay Project
- Military Scenarios
- Conclusions

Network Security – What is it?

- !!! Policy !!!
- Encryption
- AAA (Authentication, Authorization and Accounting)
- Architecture
- Confidentiality
- Prevention, Detection and Correction

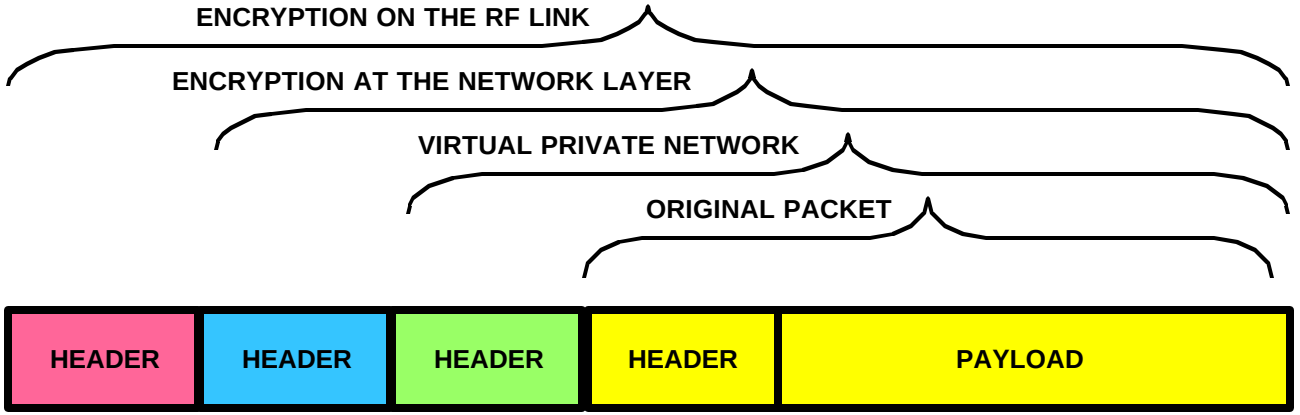
Security Truths

1. Security is necessary
2. Security is painful
   - At least to date it is
3. Security breaks everything
   - Well, enough things so that it appears to break everything
   - Lots of ingenuity required to make things work

New IETF End-to-End concept/reality is application-to-application rather than to machine-to-machine → due to middleware.

Security Truths

- Security ↑ Bandwidth Utilization ↓
- Security ↑ Performance ↓
- Tunnels Tunnels Tunnels and more Tunnels
- Performance ↓ Security ↓
  ⇒ User turns OFF Security to make system usable!
- Thus, we need more bandwidth to ensure security.



Mobile and Wireless Networks

What Do We Mean?

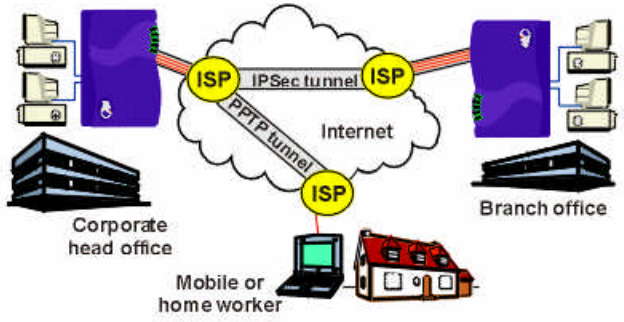
Entire Networks in Motion - Mobile Router (One View)

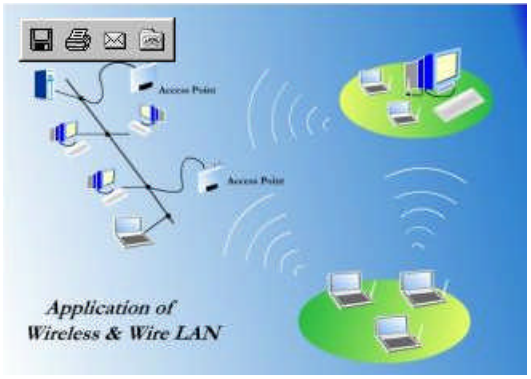
Mobile Network (Another View)

- Mobile users rather than mobile networks
- VPNs
- Dial-In
- Wireless LANs
- DHCP

⇒ This is what the corporate user of the airborne Internet "sees" as mobility

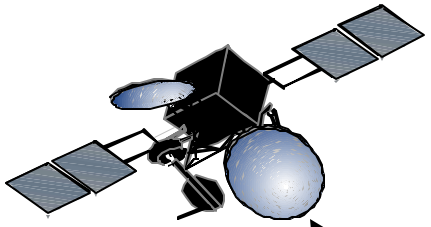
⇒ This is the cabin environment

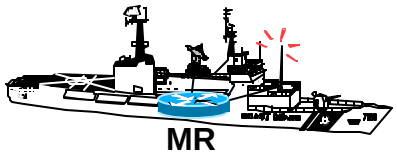




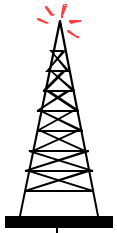
Issues and Challenges

Shared Infrastructure

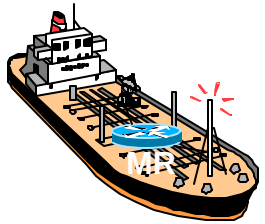




Canadian Coast Guard

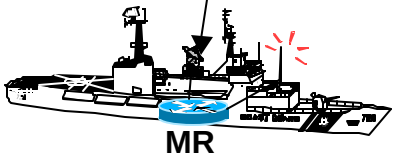


FA



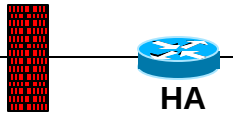
ACME Shipping

FA

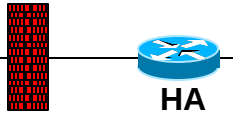


US Coast Guard

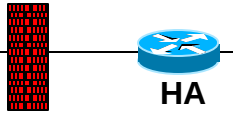
Public Internet



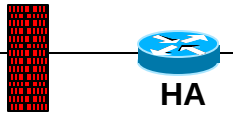
HA



HA



HA



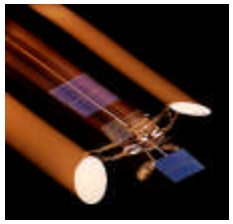
HA

ACME SHIPPING

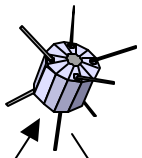
US Navy

If I run encryption on the wireless links, it will be very difficult to share infrastructure – Policy and Architecture

Asymmetrical Pathing



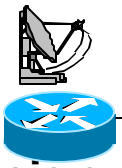
DVB Satellite



MilStar, Globalstar, Others

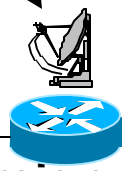
Bi-directional links are often assumed. Unidirectional links can be problematic for encryption and AAA.

Mobile Router



Foreign Agent

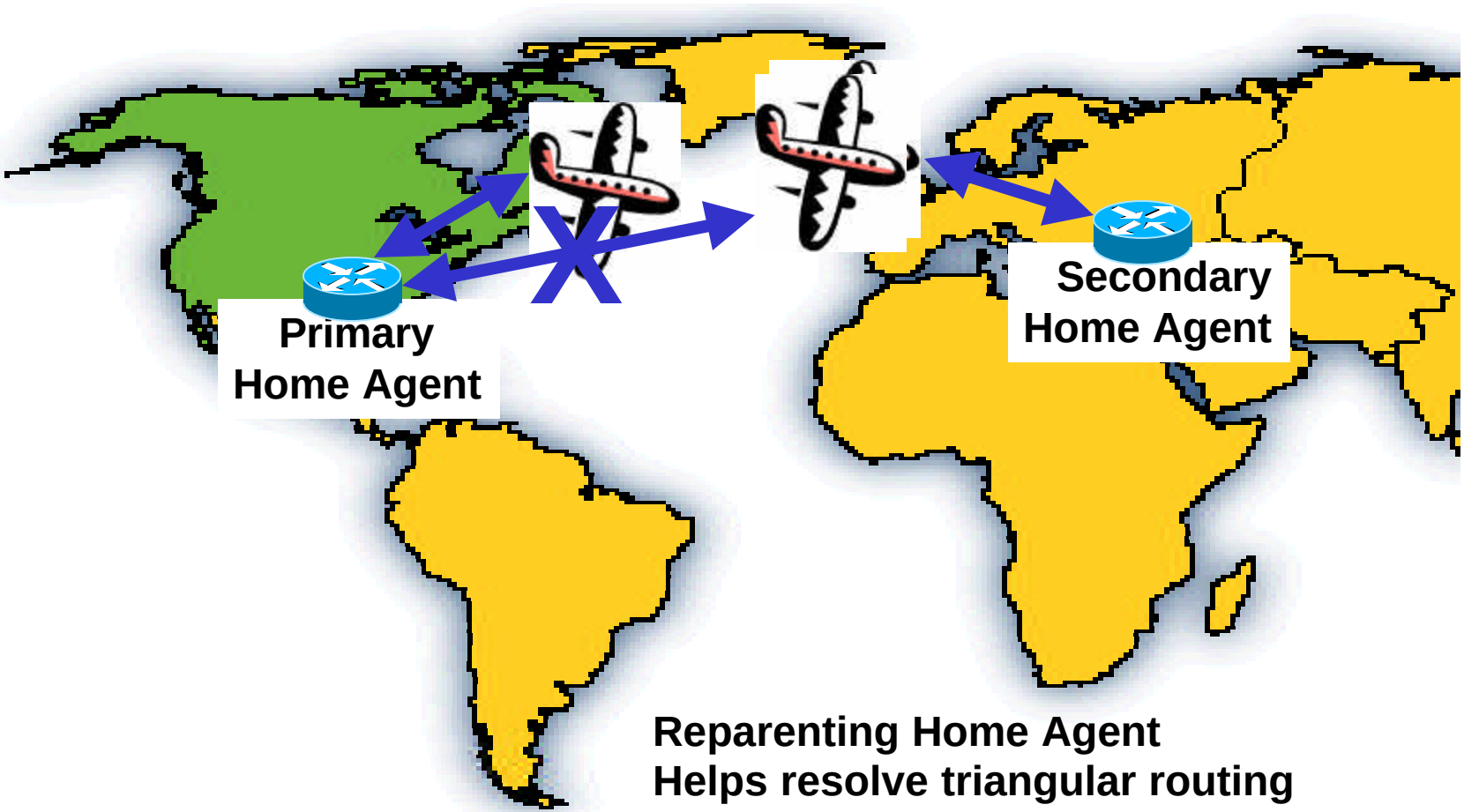
Internet



Foreign Agent

Home Agent

Reparenting the HA in Mobile-IP



Reparenting Home Agent
Helps resolve triangular routing
Problem over long distances

Encryption associations break
when handing off between networks ☹

Key Distribution

- Painful
- Difficult
- Needs to be worked to be more manageable and scalable
- Problem grows as network grows
- Sharing infrastructure makes the problem more difficult
- Military key distribution is even worse

Fortunately, this problems is being addressed by industry ☺

Middleware

- Firewalls
- Network Address Translators (NATs)
- Performance Enhancing Proxies
- Load Sharing Devices
- Traffic Shapers
- Web Accelerators
- Transparent Proxies
- Normalizers

Middleware

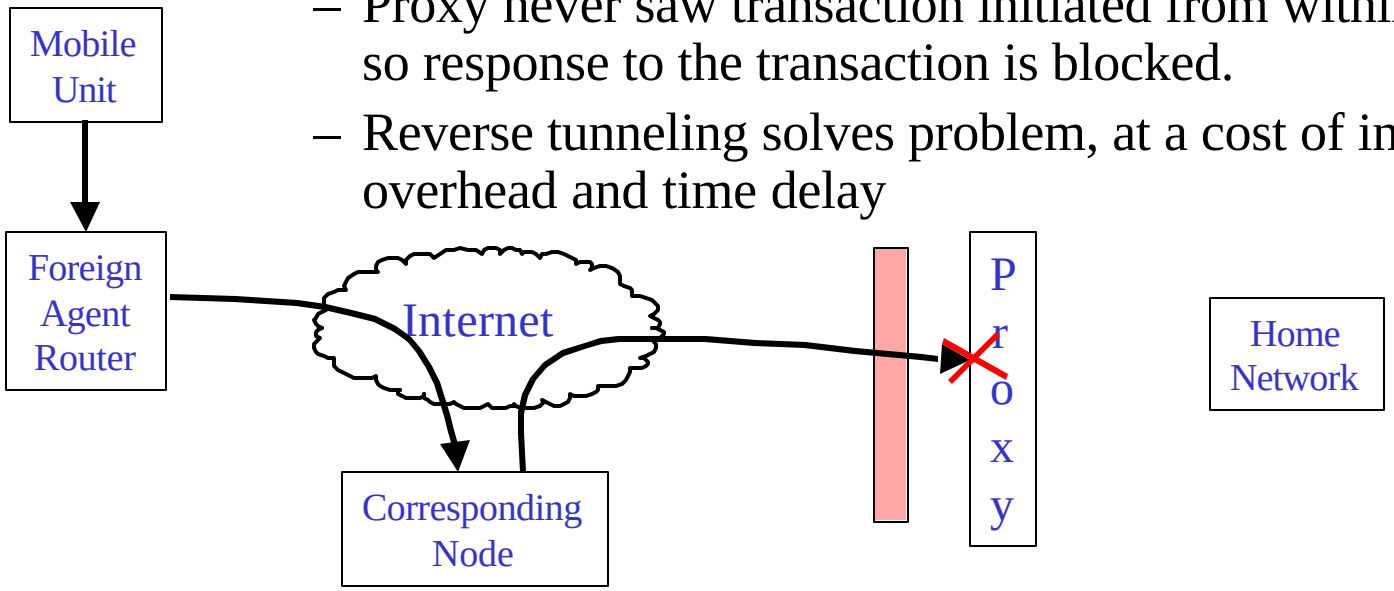
- Middleware is a reality and it doesn't appear to be going away. Rather its use is increasing – particularly with regard to network security
- This patchwork of "goop" we're putting in the network may be degrading the performance of the network.
- It is defiantly degrading our ability to figure out what is wrong with the network.
- We need to consider how the architecture should be changed to meet some of the challenges the network faces today that were not issues when the original vision was developed.
  - Deep thinking on architectural principles for the new millennium.

Example #1

- GRC personnel ran what appeared to be a complete successful transaction from inside the GRC firewall to a machine at BBN that was outside the GRC firewall.
  - Problem was that the BBN machine had been turned off for six months!
  - GRC proxy spoofed the transaction.
    - So you thought you sold you ENRON shares before it tanked, but you were wrong – only, you didn't know it until it was to late.
    - Or, you thought you sent a successful command to the aircraft, but you were wrong ☹
  - The Network Researchers say something is wrong, it is broken.
  - The Security Implementers say that is the way it is suppose to work.

Example #2

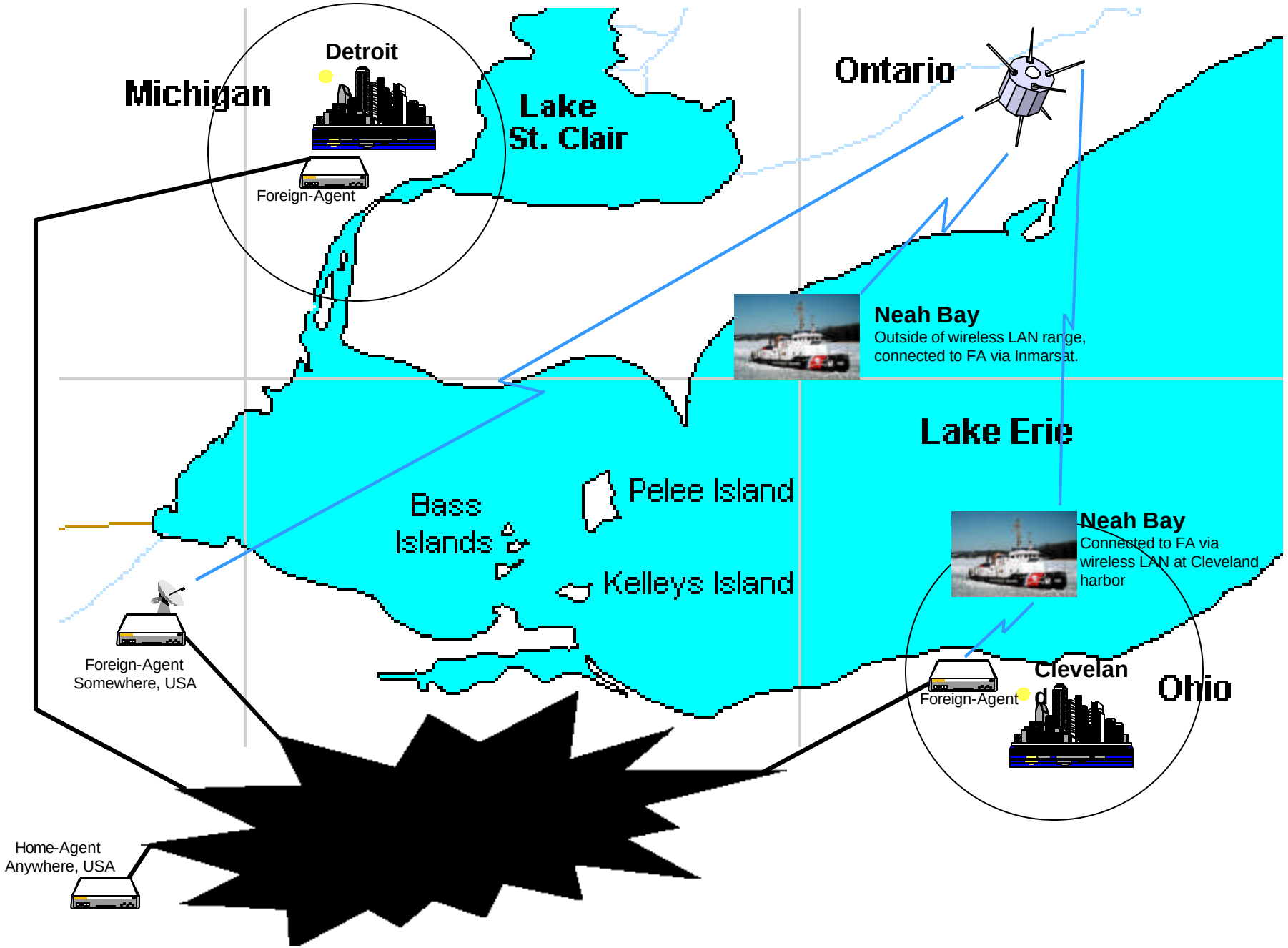
- Mobile-IP using IPv4
  - GRC firewall blocks UDP traffic
    - Need to open UDP port 436
      - Security Issue (Policy)
  - Triangular routing squashed at GRC proxy/NAT
    - Responses to transactions that originated outside the firewall are blocked by the proxy/NAT which is holding state.
      - Proxy never saw transaction initiated from within GRC network, so response to the transaction is blocked.
      - Reverse tunneling solves problem, at a cost of increased overhead and time delay



Middleware and Encryption

- Encryption renders most (if not all) Performance Enhancing Proxies (PEPs) useless relative to the encrypted flow.
- Many types of encryption make QoS engineering problematic
  - Protocol header bits hidden (IP in IP)
  - TOS header bits may be hidden

Neah Bay / Mobile Router Project

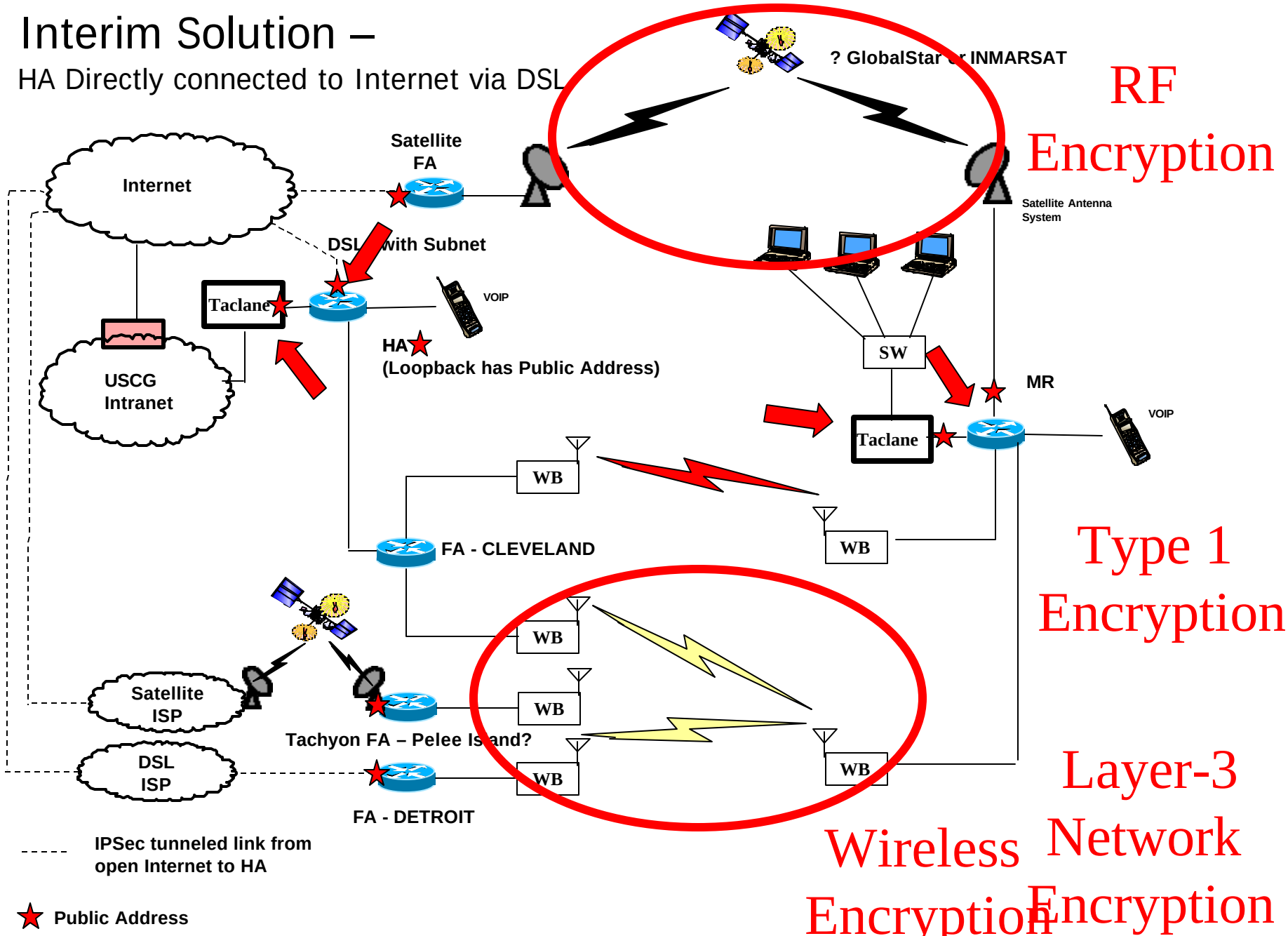


Security Issues Being Addressed

- Shared Infrastructure
- Wireless LAN Security
  - Advancements to WEP
- Mixed Address Space
  - NATs and Proxies
- Low Rate Links
- Satellite Links
- Performance over multiple tunnels
- Manageable and Scaleable Architecture

Interim Solution –

HA Directly connected to Internet via DSL

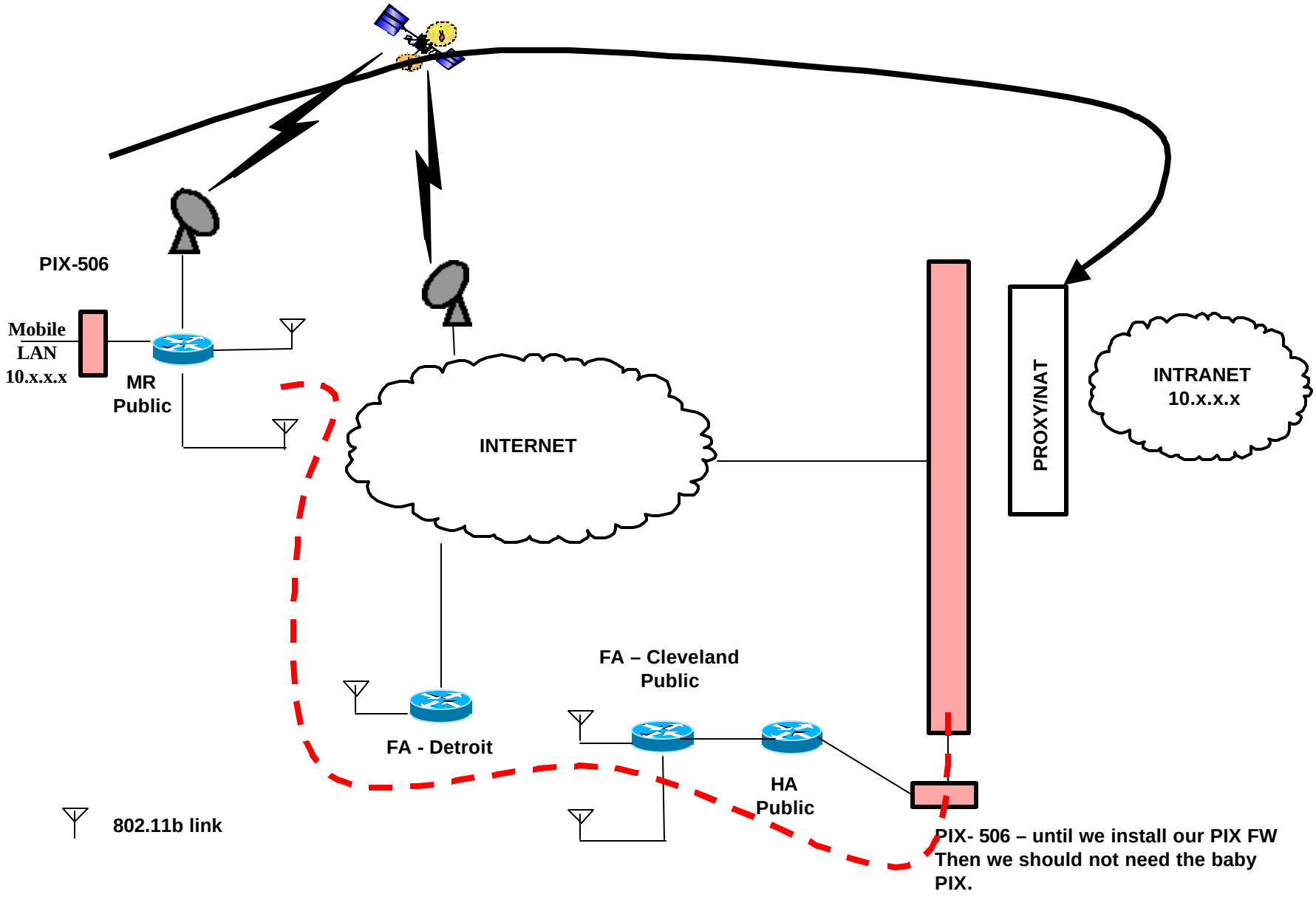


RF Encryption

Type 1 Encryption

Layer-3 Network Encryption

Wireless Encryption

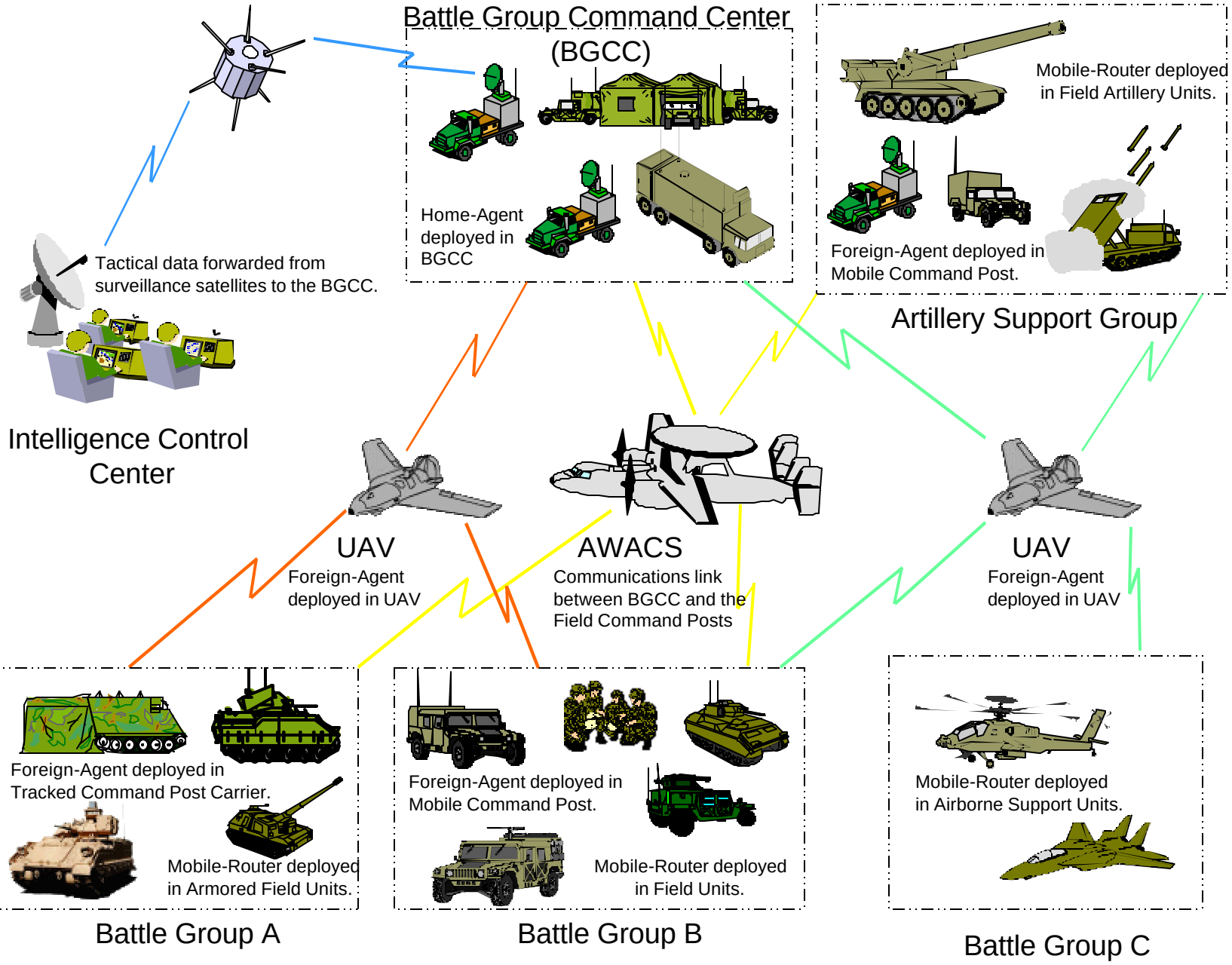

PIX-506
Mobile
LAN
10.x.x.x
MR
Public
INTERNET
PROXY/NAT
INTRANET
10.x.x.x
FA – Cleveland
Public
FA - Detroit
HA
Public
802.11b link
PIX- 506 – until we install our PIX FW
Then we should not need the baby
PIX.

Protect the MR LAN

- Firewall between MR LAN and MR as well as HA and Private Intranet
- Tunnels necessary between FAs on Internet and Firewall to provide connection of private address space over public Internet.
- Reverse tunneling required as requests from MR LAN hosts must pass through Proxy inside main firewall.

HA Outside/Collocated with Main Firewall

- Firewall between MR interfaces and public Internet as well as FA interfaces connecting to the private Intranet and the HA and Private Intranet.
- Multiple VPNs required. One for each possible interface combination.
- Tunnels necessary between FAs on Internet and Firewall to provide connection of private address space over public Internet.
- Reverse tunneling required as requests from MR LAN hosts must pass through Proxy inside main firewall. VPNs take care of this.



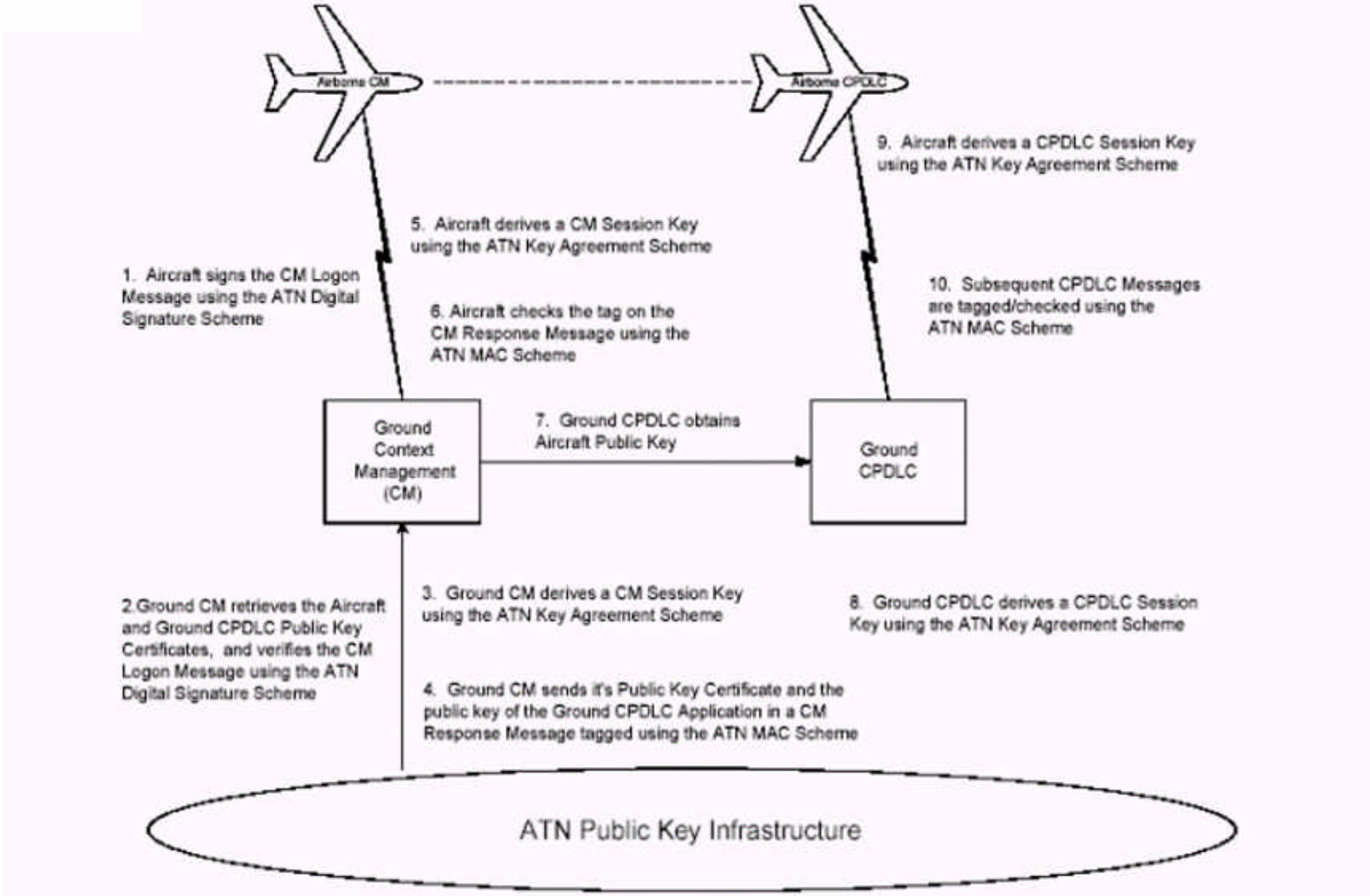
Military Applications

ATN Security Notes

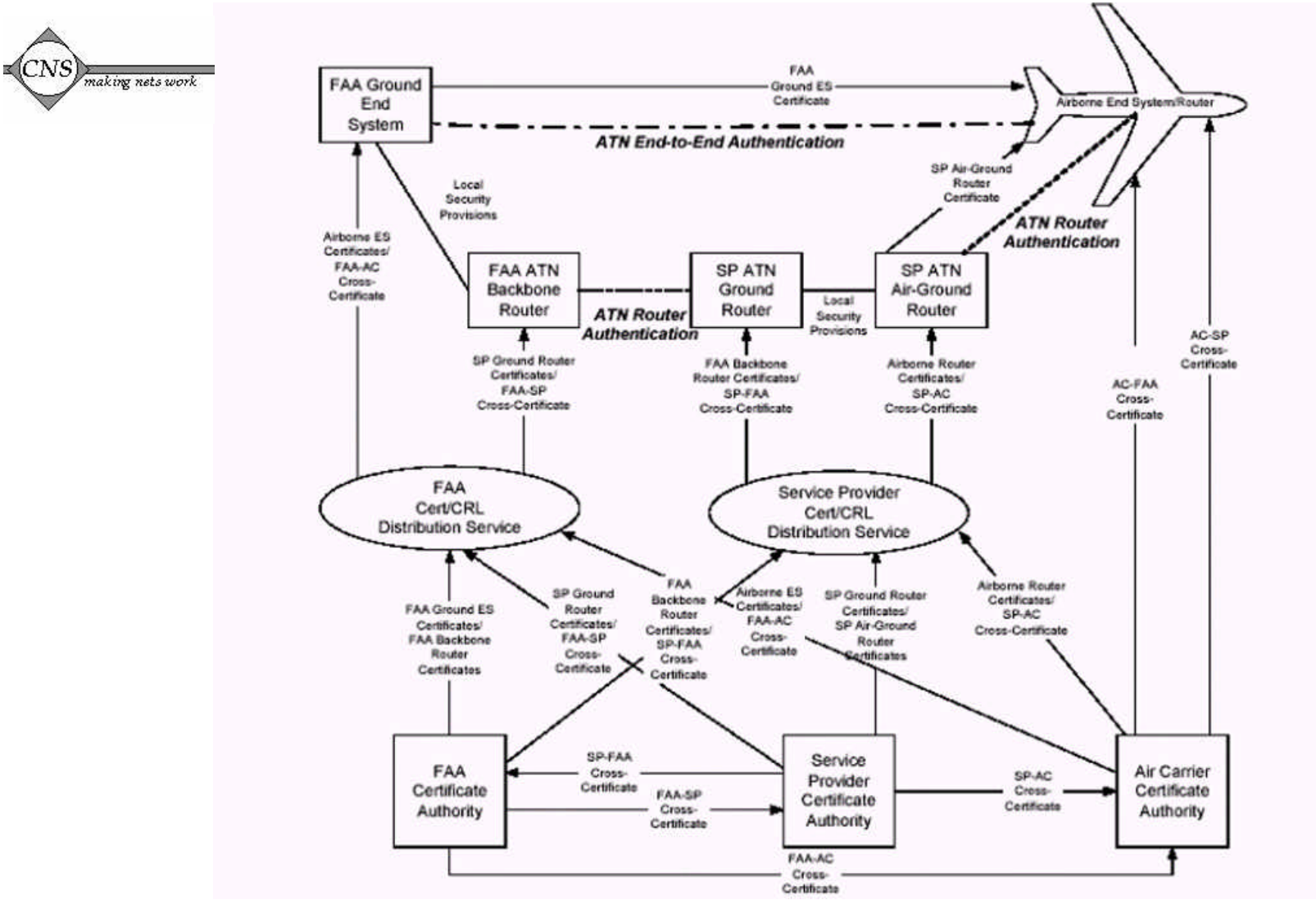
- Encryption
  - Still under development
  - Asymmetric Cryptography (Public/Private Keys)
    - Session Specify Secret Key (variant of Diffie-Hellman)
- Message Authentication
  - HMAC, IETF RFC 2104
  - Hash Function(Secure Hash Algorithm Revision One NIST)
- Authentication
  - Digital Signature (elliptic curve variant of Digital Signature Algorithm)
  - Hash Function
  - Asymmetric Enciphered (private key)
  - Certificate Authority
  - Cross-certificates

Example of Cryptographic Services

Can CPDLC bandwidth handle encryption and AAA?



Example of Certificate Environment



Conclusions

- Security is necessary, albeit often painful
- Key distribution and AAA methods need to be developed that ease the deployment
- We need to be aware of middleware
- Increased security requires increased bandwidth and connectivity
- A mobile networks means different things to different people
  - Mobile user
  - Entire networks in motion
- To much security may result in less security
  - Security bypassed for the sake of performance!